

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)524 South Walnut Street, Troy, Ohio, 45373
(including all outbuildings, curtilage, and vehicles parked
on the premises)

Case No.

3:18mj300

FILED
RICHARD W. NAGEL
CLERK OF COURT
2018 APR 12 PM 4:32
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A-4

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

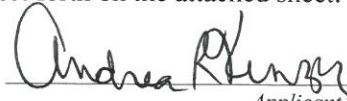
Code Section

See Attachment C-4

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

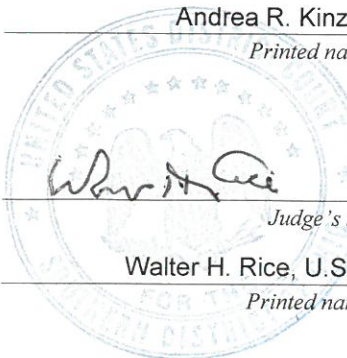
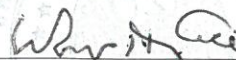
Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 4-12-18

City and state: Dayton, Ohio

Judge's signature

Walter H. Rice, U.S. District Court Judge

Printed name and title

ATTACHMENT A-4

DESCRIPTION OF LOCATION TO BE SEARCHED

524 SOUTH WALNUT STREET, TROY, OHIO, 45373 ("SUBJECT PREMISES-2") is a single family, two story residence with white siding and a wooden front deck. The street address numbers are black in color and affixed to the residence next to the front door. The SUBJECT PREMISES-2 is located on the west side of South Walnut Street between East Simpson Street and Raper Street. The SUBJECT PREMISES-2 includes all outbuildings, curtilage, and vehicles parked on the SUBJECT PREMISES-2.



ATTACHMENT B-4

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt, distribution, attempted receipt, and attempted distribution of child pornography) and 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted of child pornography), including but not limited to the following:

Computers and Electronic Media

1. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data - - whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.
8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone), tablets, and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records and Physical Records

9. Any records related to the possession, attempted possession, receipt, attempted receipt, distribution, and attempted distribution of child pornography.
10. Any images or videos of child pornography.
11. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
12. Any Internet history indicative of searching for child pornography.
13. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.
14. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.
15. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
16. Evidence of utilization of the account name rabbithole45373.
17. Evidence of utilization of the Kik messenger application.
18. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
19. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials.
20. Records of address or identifying information for individuals using computers located at the SUBJECT PREMISES-2 and any personal or business contacts or associates of his, (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords.
21. Any books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

22. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
23. Lists of computer and Internet accounts, including user names and passwords.
24. Any information related to the use of aliases.
25. Documents and records regarding the ownership and/or possession of the items seized from the SUBJECT PREMISES-2.
26. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.
27. Any GPS, mapping, and location information.

Photographs of Search

28. During the course of the search, photographs of the SUBJECT PREMISES-2 may also be taken to record the condition thereof and/or the location of items seized from the residence.

ATTACHMENT C-4

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt, Attempted Receipt, Distribution, and Attempted Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt, Attempted Receipt, Distribution, and Attempted Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents and investigators of the Commonwealth of Kentucky Office of the Attorney General, Ohio Bureau of Criminal Investigation, and FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by an individual utilizing the user name of “rabbithole45373” on a smartphone instant messenger application – namely, the Kik messenger application. This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. The residential property located at 3816 East Third Street, Apartment B, Dayton, Ohio, 45403 (hereinafter referred to as “**SUBJECT PREMISES-1**” and more fully described in Attachment A-1 hereto);
 - b. The person of **CARL LOWE**, date of birth May 14, 1975 (hereinafter referred to as “**LOWE**” and more fully described in Attachment A-2 hereto);
 - c. Cellular telephone bearing telephone number **937-540-5671** and IMSI 8901260331926604112F (hereinafter referred to as “**SUBJECT DEVICE**” and more fully described in Attachment B-3 hereto); and
 - d. The residential property located at 524 South Walnut Street, Troy, Ohio, 45373 (hereinafter referred to as “**SUBJECT PREMISES-2**” and more fully described in Attachment A-4 hereto).
3. The purpose of the Applications is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography and access with the intent to view child pornography; and violations of 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive and distribute child pornography through

interstate commerce or attempt to do so. The items to be searched for and seized are described more particularly in Attachments B-1 through B-4 hereto.

4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT PREMISES-1**, **LOWE's** person, the **SUBJECT DEVICE**, and **SUBJECT PREMISES-2**.
6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present at the **SUBJECT PREMISES-1**, on the person of **LOWE**, at the **SUBJECT PREMISES-2**, on the **SUBJECT DEVICE**, and on the computers located at the **SUBJECT PREMISES-1** and **SUBJECT PREMISES-2** and on the person of **LOWE**.

PERTINENT FEDERAL CRIMINAL STATUTES

7. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
8. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

9. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
10. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
11. For purposes of these statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:
 - a. “Actual or simulated –
 - i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
 - ii. Bestiality;
 - iii. Masturbation;
 - iv. Sadistic or masochistic abuse; or
 - v. Lascivious exhibition of genitals or pubic area of any person.”

BACKGROUND INFORMATION

Definitions

12. The following definitions apply to this Affidavit and Attachments B-1 through B-4 to this Affidavit:
 - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit

conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address

provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- g. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A “**client**” is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
- i. “**Domain Name**” refers to the common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
- j. “**Log Files**” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- n. A **“Smartphone”** is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.
- o. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.
- p. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Characteristics of Collectors of Child Pornography

13. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
 - e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Use of Computers and the Internet with Child Pornography

14. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.
- a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
 - b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites

communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.
- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Seizure of Computers

- 15. As discussed below, the investigation has determined that the **SUBJECT DEVICE**, as well as one or more computers and/or electronic storage devices located at the **SUBJECT PREMISES-1** and **SUBJECT PREMISES-2** and on the person of **LOWE**, are being used as an instrumentality in the course of, and in furtherance of, the transmission, possession, receipt, and advertisement of child pornography. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form. This includes computer hard-drives, cellular telephones and tablets, digital cameras, disks, thumb drives, CDs and other similar electronic storage devices.

16. An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.
17. Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

18. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.
19. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last modified; when was it last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.
20. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The contents of Adobe

“pdf” files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner—ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

21. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.
22. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

Persistence of Digital Evidence

23. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is “deleted” by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.
24. Typically, computer forensics focuses on at least three categories of data. These are: 1) **active data** – such as current files on the computer, still visible in file directories and available to the software applications loaded on the computer; 2) **latent data** – such as deleted files and other data that resides on a computer’s hard drive and other electronic

media in areas available for data storage, but which are usually inaccessible without the use of specialized forensic tools and techniques; and 3) archival data – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

25. **Active data** includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.
26. **Latent data** includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.
27. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

Conclusion Regarding Forensic Analysis Procedures

28. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location computers, electronic storage devices, and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.
29. Therefore, it is respectfully requested that the warrant sought by this application authorize the seizure and search of all "computer hardware," "computer software" and other computer-related documents and information found at the **SUBJECT PREMISES-1**, at the **SUBJECT PREMISES-2**, on the person of **LOWE**, and on the **SUBJECT DEVICE**, which are more fully set-out and explained herein and Attachments B-1

through B-4, and further authorize a full physical and forensic examination of the seized items at a secure location.

Craigslist

30. Craigslist is a classified advertisements website located at www.craigslist.org. It was founded in 1995, and its headquarters is currently located in San Francisco, California.
31. Users can post advertisements to various sections of the Craigslist website, including Jobs, Housing Personals, For Sale, Items Wanted, Services, Community, Gigs, Resumes, and Discussion Forums. Craigslist serves more than 700 local sites in 70 countries, and users are able to designate the geographic area to which they post their advertisements. All Craigslist postings are free of charge except for certain designated sections, including Job Postings in selected areas, Brokered Apartment Rentals in the New York City area, Therapeutic Services in the United States, Tickets By-Dealer in the United States, and Cars/Trucks By-Dealer in the United States.
32. Users of the Craigslist website can create a personalized account on the website or post advertisements without an account. Users can post advertisements to one category in one city no more than once every 48 hours. There are various life spans that determine how long advertisements are posted before they expire, depending on the category type and city. Advertisements can be renewed and re-posted after a 48-hour period, which moves the advertisements up to the top of the list.
33. When submitting postings, users are requested to provide their email address. There are three options for how users can receive responses:
 - a. Users can use an anonymized email system referred to as Craigslist 2-way email relay. Emails are routed through a craigslist.org email address and relayed to the users' actual email address. This email system is designed to protect users from spam and scams. When replying to a post, a user will see an email address such as abcde-0123456789@salae.craigslist.org. When answering an email, users will see an email such as rcc91a26d7534400a6a03514c34f9200@reply.craigslist.org. However, users still use their email program like they normally would to send and receive messages.
 - b. Users' email addresses can appear in the posting so that the actual email address is displayed and responses are received directly to the email address.
 - c. Users can provide other contact information to be displayed in the body of the post so that responses are received via a means other than email (such as by telephone).

34. The Personals section of the Craigslist website includes various sub-categories, including Women Seeking Men, Women Seeking Women, Men Seeking Men, Men Seeking Women, Misc. Romance, and Casual Encounters. Based on my training and experience, I know that the Casual Encounters section is often used by individuals seeking others for short-term sexual relationships with others.

Kik Messenger Application

35. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
36. The Kik messenger application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
37. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. Kik Interactive Inc. does not verify this information, and as such, users can provide inaccurate information.
38. Kik Interactive Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, Kik Interactive Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. Kik Interactive Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). Kik Interactive Inc. does not store or maintain chat message content.
39. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

Common Abbreviations

40. Based on my training and experience, I know that individuals frequently use abbreviations or acronyms on the Craigslist website and when communicating with each

other on messenger applications such as Kik. Some of these abbreviations or acronyms include the following (as seen later in the Affidavit):

- a. M4MW – Term for a male seeking another male along with a woman
- b. Gf – Girlfriend
- c. Yr or Y – Year
- d. Cl – Craigslist
- e. PTHC – Pre-teen hard core
- f. Pics – Pictures
- g. Vids – Videos

FACTS SUPPORTING PROBABLE CAUSE

- 41. In January 2018, agents of the Commonwealth of Kentucky Office of the Attorney General, Department of Criminal Investigations, conducted an online investigation to identify individuals who were utilizing the Craigslist website to commit child exploitation offenses. On or around January 29, 2018, an undercover officer who will be referred to for purposes of this Affidavit as “UCO-1” observed an advertisement posted in the Casual Encounters section of the Craigslist website for the geographic location of Dayton, Ohio. The advertisement had a title of “Kinky Taboo No Limits – m4mw”. The body of the advertisement stated the following: “Looking for open minded taboo no limit kinky fun. Kik me at rabbithole45373 or email here and tell me what you like. open to anything”.
- 42. Based on UCO-1’s training and experience, he knows that the terms “taboo” and “no limits” are often used by persons seeking sexual acts over the Internet. UCO-1 also knows that individuals sometimes use these terms to solicit illegal sexual activities, including sexual activities involving minors.
- 43. On or around January 29, 2018, UCO-1 responded to the above noted Craigslist advertisement by sending a message to the rabbithole45373 Kik account. UCO-1 posed as an adult male who lived in Kentucky and had an 11-year old female child in his custody. UCO-1 and the rabbithole45373 account user exchanged messages during the approximate time period of January 29, 2018 to February 20, 2018. Below is a summary of these communications:
 - a. The rabbithole45373 account user quickly asked how old UCO-1’s daughter was

and asked if UCO-1 “played” with her. When UCO-1 identified that his purported daughter was 11 years old and that he played with her, the rabbithole45373 account user responded “Hot she still go her cherry?”.

- i. Based on my training and experience, I know that individuals involved in child exploitation activities often use the term “play” to refer to engaging in sexual activities with minors.
- b. The rabbithole45373 account user asked for pictures of UCO-1’s child. UCO-1 responded by sending a profile picture of a purported minor female child. The rabbithole45373 account user responded by stating “Cute any revealing ones”. The rabbithole45373 account user later asked UCO-1: “U got any x pics of your lil one”.
 - i. Based on my training and experience, I know that individuals often utilize terms such as “revealing”, “x”, and “x-rated” when requesting nude or sexually explicit pictures from others.
- c. The rabbithole45373 account user talked about engaging in sexual activities with his nieces and nephews. The rabbithole45373 account user stated that he engaged in sexual activities with one of his nieces and one of his nephews when they were ten years old, one of his nieces when she was six months old, one of his nieces when she was one year old, and one of his nephews during the time that he was 11 to 16 years old. The rabbithole45373 account user talked about the possibility of purchasing a drug dealer’s six-year old child and engaging in sexual activities with this child. The rabbithole45373 account user also talked about his desires to engage in sexual activities with an infant. Below are excerpts of these communications:

January 30, 2018:

Rabbithole45373: I told my sisters kids they had to stay naked when i caught them they could tell i was playing so they said i had to get that way so i did. I told em to keep playing and i wanted to play truth or dare

Rabbithole45373: After a while making them play i dared they both suck me then dared him to put it in her which he couldnt so i showed em how and busted her hymen

.....

January 30, 2018:

Rabbithole45373: i have a crackhead that would sell me her daughter for a bit but scared

Rabbithole45373: Shes 6

UCO-1: Yea I would take money but it got to be cash
Rabbithole45373: Cool and i know her daughter has been fucked
which i want a virgin

.....

January 31, 2018:

Rabbithole45373: Cool u think u could get in a baby
UCO-1: Doubt it
Rabbithole45373: Be hot to try
UCO-1: Would you
Rabbithole45373: Yes
UCO-1: My gf wants another kid
Rabbithole45373: i would pound and thrust so hard in a new born
Rabbithole45373: Do it
UCO-1: You ever done it
Rabbithole45373: u probably don't like fuckin her tho huh
Rabbithole45373: No licked one
UCO-1: How old
Rabbithole45373: u?
Rabbithole45373: 6mos
UCO-1: Her girl the only one I had
UCO-1: You don't have her now?
Rabbithole45373: I wanna penetrate a baby bad
Rabbithole45373: No shes 4 now
Rabbithole45373: How often u fuck the girl
UCO-1: Where did she go
UCO-1: Probably at least 2 or 3 nights a month
Rabbithole45373: My sisters baby.

.....

February 14, 2018:

Rabbithole45373: If i didn't think id tear the shit outta her id try my
one yr old niece and no but want to
Rabbithole45373: I did put the tip of my dick in her mouth few
months back

.....

Rabbithole45373: Nice wish u were closer id take a chance and rape
my niece with ya

.....

UCO-1: How were you gonna rape your niece if she don't
go with you

Rabbithole45373: I babysit her but no driving shit sucks

UCO-1: Yea

UCO-1: That all you done with her
Rabbithole45373: Yea
Rabbithole45373: I wanna split her open tho
Rabbithole45373: I get transfixed on her pussy when shes bein
changed
Rabbithole45373: I wanna so lay on top a baby and force my way in

.....

February 20, 2018:

Rabbithole45373: Nice im talking to a girl no that had a baby last
week and a 8 yr
UCO-1: What she ok with?
Rabbithole45373: Everything she wants a incest pedo family
UCO-1: Damn where you find her
Rabbithole45373: On here she replied to my cl ad

- d. The rabbithole45373 account user talked about videos he had in his possession depicting children. The rabbithole45373 account user indicated that he downloaded at least some of these files from the Internet. He also indicated that he used the terms “pthc” and “preteen hardcore” as search terms when seeking the files from the Internet. The rabbithole45373 account user offered to provide some of the suspected child pornography files to UCO-1 if they ever met.
- i. Based on my training and experience, I believe that the descriptions provided by the rabbithole45373 account user regarding the files he had in his position depicting children are consistent with child pornography.
- ii. Based on my training and experience, I know that “pthc” and “preteen hard core” are common terms that individuals utilize when searching for child pornography.
- iii. Below are excerpts of some of the communications between the rabbithole45373 account user and UCO-1 regarding the suspected child pornography files:

January 30, 2018:

Rabbithole45373: . . . yes ive got hot vids where infants are taking
cock
UCO-1: Nice
UCO-1: Where you get it
Rabbithole45373: Downloaded on dark web and old limewire i got a 2
yr old bein penetrated hard like 4 inches of a guys
dick

UCO-1: How I get that
UCO-1: Would trade off this girl
Rabbithole45373: On a laptop u download a dark web browser the
using it do a search for like pthc preteen hardcore
and thatll start ya off
UCO-1: My computer belongs to my job
UCO-1: Can't find on there
Rabbithole45373: Damn wish i were closer id record ya some to disk
only youd have access to
UCO-1: Yea

.....

January 31, 2018:
Rabbithole45373: Whats up
UCO-1: Working
UCO-1: U?
Rabbithole45373: Whatchin porn
UCO-1: Anything good
Rabbithole45373: Young
UCO-1: Homemade?
Rabbithole45373: No i wish
UCO-1: What's your favorite
Rabbithole45373: Infant
UCO-1: Yea I seen pics mostly
UCO-1: Hard to get
Rabbithole45373: I cherish mine

.....

January 31, 2018:
UCO-1: I been thinking about that disk you said you can
make
Rabbithole45373: Yea
UCO-1: You still want to
Rabbithole45373: I could upload to google cloud and let u see u got
any for me
UCO-1: Nothing like what we talked about
UCO-1: Do I have to download or can I put on my phone
Rabbithole45373: On phone got a g rated pic of your girl?

.....

February 20, 2018:
UCO-1: What kind of videos do you got?

Rabbithole45373: Young 2 y and up u
UCO-1: A few older ones
Rabbithole45373: Is in filmed long time ago or older stars
UCO-1: Older girls
Rabbithole45373: Oh blahhhhh i like newborn to tenish
UCO-1: Same
UCO-1: Can't download anything on my work computer
though
Rabbithole45373: Yea maybe talk some more and once comfy i may
show ya some things

- e. The rabbithole45373 account user did not communicate with UCO-1 during the approximate time period of February 1, 2018 to February 13, 2018. On or around February 14, 2018, the rabbithole45373 account user sent a message to UCO-1 stating that he had broken his phone and recently obtained a new one.
- f. During the course of the communications, the rabbithole45373 account user identified that he was 40 years old and resided in Dayton, Ohio. The rabbithole45373 account user stated that he was unable to drive because of a DUI (Driving Under the Influence) conviction.
44. Based on my training and experience, I believe that the statements made by the rabbithole45373 account user regarding the video files in his possession (as detailed above) are indicative of someone who possesses a collection of child pornography. His statements regarding the use of the search terms "pthc" and "preteen hard core", as well as his use of Limewire (a Peer-to-Peer file sharing program) and the "dark web", are consistent with someone who utilizes the Internet to obtain child pornography. I also believe that in requesting to receive "revealing" or "x" pictures of UCO-1's purported 11-year old daughter, the rabbithole45373 account user was attempting to receive child pornography. Furthermore, based on his offer to provide video files to UCO-1 on a disk if they ever met, I believe that the rabbithole45373 account user was attempting to distribute child pornography.
45. During the course of the investigation, two administrative subpoenas were served to Kik Interactive Inc. requesting subscriber information for the rabbithole45373 account, as well as logs of IP addresses utilized to access the account and transmit messages. The subpoenas were served to Kik Interactive Inc. on or around February 1, 2018 and February 26, 2018. Records received from Kik Interactive Inc. in response to the subpoenas provided the following information:
- a. The rabbithole45373 account was created on or around November 17, 2017. The profile name for the account was "Chad Thomas", and the email address mgage45373@gmail.com was associated with the account profile.

- b. The account was last accessed on or around February 21, 2018. Most of the IP addresses utilized to access the account were serviced by the T-Mobile network. This activity is consistent with someone whose cellular telephone provider is T-Mobile and who uses the data plan from his/her cellular telephone to access the Internet.
 - c. A Metro PCS Model LGMP260 android device was used to access the account on or around December 4, 2017.
46. On or around January 31, 2018, an administrative subpoena was served to Craigslist requesting information related to the advertisement to which UCO-1 responded. On or around February 15, 2018, Craigslist provided information in response to the subpoena. These records identified that the poster of the advertisement utilized the email address carlwlowe937@gmail.com and the telephone number **937-540-5671** (the number for the **SUBJECT DEVICE**).
47. T-Mobile was identified as the service provider for telephone number **937-540-5671**. On or around February 23, 2018, an administrative subpoena was served to T-Mobile requesting subscriber information for this account. T-Mobile provided records in response to the subpoena on or around February 27, 2018. These records identified that during the approximate time period of July 12, 2017 to the present, the telephone was subscribed to **LOWE**. The service and billing addresses were initially listed as 329 Ernst Avenue in Dayton, Ohio. On or around January 5, 2018, the billing and service addresses were changed to 4317 Bayberry Cove in Bellbrook, Ohio.
48. On or around March 20, 2018, T-Mobile was served with an additional administrative subpoena requesting subscriber information for telephone number **937-540-5671** and information regarding the device that utilized this telephone number. T-Mobile provided records in response to the subpoena on or around March 21, 2018. These records identified that the telephone number continued to be subscribed to by **LOWE**, with the billing and service address in Bellbrook, Ohio. The records also identified that effective on or around March 5, 2018, telephone number **937-540-5671** was utilized by an LG K20 Plus cellular telephone bearing International Mobile Subscriber Identity (IMSI) 310260332660411 and device number 352130097307309.
- a. Based on Internet research, I have determined that a Metro PCS Model LGMP260 android device (the android device utilized to access the rabbithole45373 Kik account) is a LG K20 Plus cellular telephone.
49. On or around February 19, 2018, Google Inc. was served with a search warrant requesting information associated with the Google accounts carlwlowe937@gmail.com (the account associated with the Craigslist advertisement to which UCO-1 responded) and mgage45373@gmail.com (the account associated with the rabbithole45373 Kik account). Google Inc. provided records in response to the search warrant on or around March 21, 2018. These records included subscriber information and the contents of the

two email accounts. Review of the records for the carlwlowe937@gmail.com email account provided the following information:

- a. The account was created on or around February 19, 2016, using the name “carl l”. The account was logged into as recently as February 7, 2018.
 - b. At least approximately twelve of the email messages received by the carlwlowe937@gmail.com account were addressed to **CARL LOWE**.
 - c. Approximately four of the email messages received by the carlwlowe937@gmail.com account contained receipts from the Uber taxi service application. Two of the receipts indicated that the account user was picked up or dropped off at 3819 East Third Street in Dayton, Ohio, and the other two receipts indicated that the account user was picked up or dropped off at 3822 East Third Street in Dayton, Ohio.
 - i. I have determined that both of these addresses are less than 20 feet away from the **SUBJECT PREMISES-1**.
 - d. In approximately five of the email messages, the carlwlowe937@gmail.com account user appeared to be communicating with other individuals regarding advertisements on the Craigslist website.
 - e. On or around February 5, 2018, a message was received from the carlwlowe937@gmail.com account from the Google website. This email message notified the carlwlowe937@gmail.com account user that a new device had been utilized to access the email account – that being a ZTE Majesty Pro LTE cellular telephone.
 - f. Approximately eight messages were received by the carlwlowe937@gmail.com account from email addresses associated with Frontier Communications. Some of these messages indicated that the carlwlowe937@gmail.com account user had created an Internet account with Frontier Communications in late January 2018.
 - g. Approximately one email message was received by the carlwlowe937@gmail.com account from an email address associated with QLink Wireless. This email message indicated that the carlwlowe937@gmail.com account user had a telephone account with QLink Wireless.
50. Review of the records provided by Google for the mgage45373@gmail.com email account provided the following information:
- a. The account was created on or around June 2, 2017, using the name “ejrkw ddiddrruduGage”. The account was logged into as recently as February 17, 2018.

- b. In approximately eight of the email messages, the mgage45373@gmail.com account user appeared to be communicating with other individuals regarding advertisements on the Craigslist website. In some of these messages, the mgage45373@gmail.com account user appeared to make comments about an interest in juveniles. For example, on or around December 18, 2017, the mgage45373@gmail.com account user sent an email to another individual stating the following: "You like young too?" Also for example, on or around December 14, 2017, the mgage45373@gmail.com account user sent an email to another individual stating the following: "Whats up what taboo you like most. Incest and young here".
 - c. In approximately two of the sent email messages, the mgage45373@gmail.com account user requested that the recipient of the messages contact him via Kik Messenger at the rabbithole45373 account.
 - d. On or around February 1, 2018, the mgage45373@gmail.com account user received a message that provided a notification regarding the shipment of a ZTE Z798BL GSM Handset SIM 5 device. The notification stated that the device was being shipped to Mary Lowe at the **SUBJECT PREMISES-2**.
 - i. Based on Internet research I have determined that a ZTE Z798BL device is a ZTE Majesty Pro cellular telephone. As noted above, the records from Google indicated that this same make and model of cellular telephone was utilized to access the carlwlowe937@gmail.com account.
 - ii. As further detailed below, the investigation has determined that Mary Lowe is **LOWE**'s sister.
51. Based on the email messages that the carlwlowe937@gmail.com account received from Frontier Communications (as detailed above), an administrative subpoena was served to Frontier Communications on or around March 27, 2018 requesting information related to any Internet accounts in **LOWE**'s name and/or associated with the email address carlwlowe937@gmail.com. Records received from Frontier Communications in response to the subpoena identified that there is currently an Internet account in **LOWE**'s name at the **SUBJECT PREMISES-2** (the same address where the ZTE Majesty Pro telephone was shipped, as detailed above). The records identified that the Internet account was activated on or around January 26, 2018.
52. Based on my training and experience, I know that individuals often utilize variations of their first, middle, and last names in their email addresses. Based on the use of the email address of carlwlowe937@gmail.com and the subscriber name of **CARL LOWE** identified in T-Mobile's records, I conducted a search of public records and law enforcement databases for individuals with the name of **CARL W. LOWE** who reside in Montgomery County, Ohio. I identified that there is a **CARL WAYNE LOWE** who is

currently required to register as a sex offender and who lists the **SUBJECT PREMISES-1** on his current sex offender registration paperwork. **LOWE** is presently 42 years old.

- a. As detailed above, the rabbithole45373 account user identified that he was 40 years old. Based on my training and experience, I know that individuals involved in child exploitation offenses often do not provide completely accurate information regarding their identities when communicating with others in order to avoid possible detection by law enforcement officers.
53. Based on review of records from the Montgomery County, Ohio Court of Common Pleas, I have determined that **LOWE** was convicted in January 2016 of one count of Pandering Sex Oriented Material Involving a Minor, in violation of Ohio Revised Code (O.R.C.) Section 2907.322, one count of Pandering Obscenity Involving a Minor, in violation of O.R.C. Section 2907.321, and one count of Possession of Criminal Tools, in violation of O.R.C. 2923.24. The conviction relates to child pornography files that were recovered from computers seized from **LOWE**'s residence in February 2014. **LOWE** was sentenced to five years of probation. As a result of this conviction, **LOWE** was required to register as a Tier II sex offender (which requires registration for a period of 25 years).
 54. As part of the investigation, I have contacted **LOWE**'s current Probation Officer. The Probation Officer provided the following information:
 - a. **LOWE** has reported to the Probation Officer that he resides alone at the **SUBJECT PREMISES-1**.
 - b. The conditions of **LOWE**'s probation prohibit him from possessing computers and cellular telephones that have access to the Internet. **LOWE** has reported to the Probation Officer that he does not have any such devices and does not have a cellular telephone.
 - c. As part of supervising **LOWE**, the Probation Officer has gathered information regarding **LOWE**'s family members. The Probation Officer identified that **LOWE** two sisters, one of whom is Mary Lowe. **LOWE** has reported to the Probation Officer that Mary Lowe has seven children.
 - i. As part of the investigation, I have determined the approximate ages of these children. The approximate ages of some of the children are consistent with the approximate ages of the nieces and nephews that the rabbithole45373 identified in his communications with UCO-1.
 - ii. Records from the Ohio Bureau of Motor Vehicles identified that Mary Lowe utilizes the **SUBJECT PREMISES-2** on her current Ohio driver's license and on the registration information for two motor vehicles.

- d. As part of the terms of **LOWE**'s probation, the Probation Officer is permitted to search **LOWE**'s residence. The Probation Officer noted that there were a number of previous occasions in which she attempted to search the **SUBJECT PREMISES-1**, but **LOWE** did not answer the door. The Probation Officer suspected that **LOWE** was inside the residence on one or more of these occasions.
 - e. On or around March 15, 2018, the Probation Officers contacted **LOWE** outside of the **SUBJECT PREMISES-1** while he was talking to one or more other individuals who were sitting in a vehicle. The Probation Officer requested to search the **SUBJECT PREMISES-1** at that time, and **LOWE** provided her with access to the residence. The Probation Officer did not locate any cellular telephones or computer devices during her search.
55. Based on my training and experience, I know that individuals who are involved in child exploitation offenses and who are prohibited by conditions of probation or parole from possessing computer devices often still possess and utilize such devices. I also know, based on my training and experience, that these individuals often undertake great efforts to conceal these devices from their probation or parole officers. Individuals often find hiding places in their residences to conceal the devices. It is also common for individuals to conceal the devices on their persons (such as in their orifices), to pass the devices off to others when approached by probation or parole officers (such as the individuals in the vehicle to whom **LOWE** was talking when approached by his Probation Officer), or to store the devices at the residences of family members or friends when they are not being used.
56. Also based on my training and experience, I know that individuals who utilize cellular telephones and electronic accounts in furtherance of illegal activities and/or who are prohibited from possessing cellular telephones often utilize fictitious names and/or billing addresses when establishing their accounts. Individuals utilize fictitious identifying information to avoid possible detection by law enforcement officers.
57. As part of the investigation, I have obtained and reviewed a report from the Dayton Police Department regarding an incident at the **SUBJECT PREMISES-1** on or around December 22, 2017. According to the report, officers of the Dayton Police Department responded to the **SUBJECT PREMISES-1** after **LOWE** reported that his friend had suffered from a possible drug overdose. When officers arrived, they communicated with **LOWE** regarding the incident. **LOWE** confirmed that he resided at the **SUBJECT PREMISES-1**, and that the friend who suffered from the possible overdose was visiting him. According to the report, officers documented that **LOWE**'s telephone number was **937-540-5671**.
58. On or around April 9, 2018, a search warrant was authorized by the United States District Court for the Southern District of Ohio for the cellular telephone assigned call number **937-540-5671** (the **SUBJECT DEVICE**). This search warrant authorized the release of

location information (i.e., cell site, cell sector, and GPS information) for the **SUBJECT DEVICE** by T-Mobile for a period of 30 days. Pursuant to the search warrant, T-Mobile began providing the requested location information for the **SUBJECT DEVICE** to the FBI during the early evening hours of April 10, 2018. T-Mobile has provided the approximate location (expressed in the latitude, longitude, and a measurement of uncertainty) of the **SUBJECT DEVICE** every approximately 15 minutes. The location information provided by T-Mobile during the time period of the evening of April 10, 2018 through the morning of April 12, 2018 provided the following information:

- a. During the overnight hours of April 10, 2018 and April 11, 2018, the **SUBJECT DEVICE** was consistently in the area of the **SUBJECT PREMISES-1**.
 - b. During the daytime hours of April 11, 2018, the **SUBJECT DEVICE** was in the area of the **SUBJECT PREMISES-1** on a number of occasions. The cellular telephone also traveled to other locations throughout the day.
 - c. The **SUBJECT DEVICE** was located in the Southern District of Ohio at all times.
59. Based on all of the information noted in the Affidavit, I submit that there is probable cause to believe that **LOWE** is the user of the rabbithole45373 Kik account, the carlwlowe937@gmail.com email account, and the mgage45373@gmail.com email account. I also submit that there is probable cause to believe that he has utilized these and possibly other accounts to communicate with others about child exploitation offenses, to view and/or possess child pornography, to receive and/or attempt to receive child pornography, and to attempt to distribute child pornography.
60. Furthermore, I submit that there is probable cause to believe that **LOWE** has recently utilized at least two cellular telephones – that being the **SUBJECT DEVICE** and the ZTE Majesty Pro cellular telephone that was shipped to the **SUBJECT PREMISES-2** – to communicate with others regarding child exploitation and child pornography offenses. Based on **LOWE**'s statements to UCO-1 about burning child pornography files to a disk, it is reasonable to believe that he possesses and/or has access to at least one desktop computer or laptop.
61. Based on my training and experience, I know that individuals typically maintain their cellular telephones on their persons and in their residences. In my experience, it is not uncommon for individuals to maintain their previously used cellular telephones after purchasing new ones in case they need data (such as contact telephone numbers) from the previous telephones. Although the Probation Officer did not locate any cellular telephones or computer devices when searching the **SUBJECT PREMISES-1** on or around March 15, 2018, I submit that it is reasonable to believe that such devices were in fact concealed inside the residence, on **LOWE**'s person, or in his associate's vehicle. In fact, recent location data for **SUBJECT DEVICE** shows it has consistently been in the

vicinity of **SUBJECT PREMISES-1** over the approximately past two days.

62. Based on the email messages recovered from the two Google accounts and the records from Frontier Communications (as detailed above), it appears that **LOWE** established an Internet account at the **SUBJECT PREMISES-2** and shipped a ZTE Majesty Pro cellular telephone to this residence. In his Kik communications with UCO-1, **LOWE** identified that he engaged in sexual activities with his nieces and nephews and that he baby-sat one of his nieces. Based on this and other information noted in the Affidavit, it is reasonable to believe that **LOWE** periodically spends time at the **SUBJECT PREMISES-2**, utilizes computer devices at the **SUBJECT PREMISES-2**, and potentially stores computer devices at the **SUBJECT PREMISES-2**.
63. Based on all of the information noted in the Affidavit, there is probable cause to believe that the **SUBJECT DEVICE** and one or more computer devices are currently located at the **SUBJECT PREMISES-1**, at the **SUBJECT PREMISES-2**, and/or on **LOWE's** person, and that these devices contain evidence of **LOWE's** child exploitation and child pornography offenses. There is also probable cause to believe that various documents and records related to **LOWE's** computer devices and child exploitation activities are located at the **SUBJECT PREMISES-1**, at the **SUBJECT PREMISES-2**, and/or on **LOWE's** person.
64. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices to possess, receive, and advertise child pornography and to discuss the sexual exploitation of children. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.
65. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons.
66. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons.
67. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence

typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).

68. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
69. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.
70. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chat rooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
71. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.
72. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.

73. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.
74. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.
75. Based on my training and experience, I know that providers of cellular telephone service (such as T-Mobile) and Internet Service Providers (such as Frontier Communications) often send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. Individuals often maintain these documents in their residences and/or on their computers. These documents can be materially relevant to investigations of child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.
76. Also based on my training and experience, I know that individuals often maintain the boxes, shipping documents, instruction manuals, and paraphernalia for the computer devices that they purchase. These items are maintained for a variety of reasons, including for reference for device instructions, for possible warranty information, and in the event that the devices need to be returned. These items can be materially relevant to investigations of child exploitation offenses in that they provide evidence of the computer devices utilized in furtherance of the crimes.

\\

\\

\\

\\

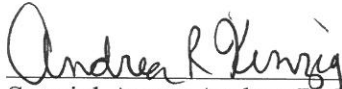
\\

\\


\\

CONCLUSION

77. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the **SUBJECT PREMISES-1**, on the person of **LOWE**, at the **SUBJECT PREMISES-2**, on the **SUBJECT DEVICE**, and on the computers located at the **SUBJECT PREMISES-1** and **SUBJECT PREMSISES-2** and on the person of **LOWE**, in violation of 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1).
78. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-4.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 12th of April, 2018


HONORABLE WALTER H. RICE
UNITED STATES DISTRICT COURT JUDGE